



Office 365 Business Premium/E1/E3/E5 をご利用中のユーザー様向け

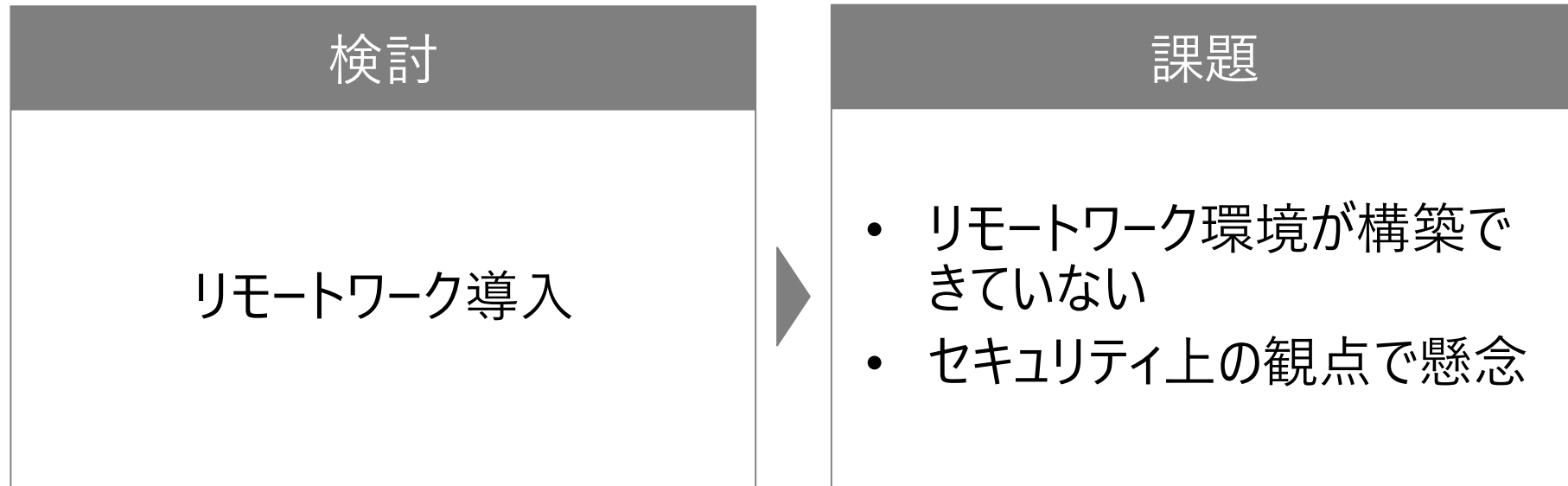
# Microsoft 365 で簡単に実現できる 自宅 PC を使った安全なリモートワーク環境

日本マイクロソフト株式会社



はじめに

## セキュアリモートワークの実施にむけて



**自宅 PC でも Office 365 を安全に利用することができ、  
リモートワークが実現できます！**

ご準備いただくもの



Office 365 Business Premium/E1/E3/E5



追加



Enterprise Mobility + Security E3



Microsoft Cloud App Security



Microsoft Defender ATP

# Microsoft 365 で実現できる安全なリモートワークの 3 つのアクション



## ① Office 365 からダウンロード禁止、自宅に機密情報を残さない

### Microsoft Cloud App Security



- Office 365 からのデータのダウンロードを禁止する (制限された Web アクセス)
- 画面の切り取り／コピー／貼り付け／印刷をブロックする (制限された Web アクセス)
- Office 365 へのデータのアップロードを禁止する (制限された Web アクセス)

## ② 管理された端末からのみのアクセス制限を実施

### Azure Active Directory P1



- 管理された端末からのみのアクセスを許可する
- 管理されていない端末が Office 365 にアクセスする場合には、制限された Web アクセスのみを許可するポリシーを適用

## ③ 端末がマルウェアに感染しても AI が検知・除去

### Microsoft Defender ATP



- AIを活用して、24時間365日脅威を検知・除去まで行う
- 管理者はダッシュボードからユーザーの端末が感染しているか確認可能

※企業所有の Windows 10 PC を持ち出してご利用いただく際の推奨シナリオとなります。

# ご提案プラン

## 推奨構成プラン

※本ガイドのすべての手順が対象

## 最小構成プラン

※本ガイドの P.30-59 の手順が対象

ダウンロード禁止	✓	✓
画面の切り取り／コピー／ 貼り付け／印刷をブロック	✓	
アップロード禁止	✓	
アクセス制限	✓	✓
デバイスの保護	✓	

## 推奨構成プラン 編

※本ガイドのすべての手順が対象となります。

# Enterprise Mobility + Security E3

- Azure Active Directory Premium P1
- Microsoft Intune

Microsoft Cloud App Security

Microsoft Defender ATP



# 設定手順 (概要)

## ① Azure AD の条件付きアクセスを設定して、セッション制御を有効にする

※セッション制御の対象はブラウザ利用時のみとなります。非管理 PC の Office アプリからのアクセスをブロックしたい場合は後述の P.52 以降をご参照ください。

※セッション制御の対象はブラウザ利用時のみとなります。非管理 PC の Teams クライアントからのアクセスをブロックしたい場合は後述の P.60 以降をご参照ください。

※社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

## ② Microsoft Cloud App Security でセッション制御が有効化になっていることを確認する

## ③ Microsoft Cloud App Security で 3つのセッションポリシーを設定する

- ・ダウンロードのブロック (制限された Web アクセス)
- ・切り取り/コピー/貼り付けのブロック (制限された Web アクセス)
- ・アップロードのブロック (制限された Web アクセス)

## ④ Microsoft Defender ATP を設定する

※企業所有の Windows 10 PC を持ち出してご利用いただく際の推奨シナリオとなります。

## ① Azure AD の条件付きアクセスでセッション制限を有効化

1. ブラウザー画面を開き、Azure Active Directory 管理センターの URL <https://aad.portal.azure.com> にアクセスします。
2. Azure Active Directory 管理センター画面で、[Azure Active Directory] - [セキュリティ] - [条件付きアクセス] の順にクリックします。
3. 条件付きアクセス画面で、[新しいポリシー] をクリックします。

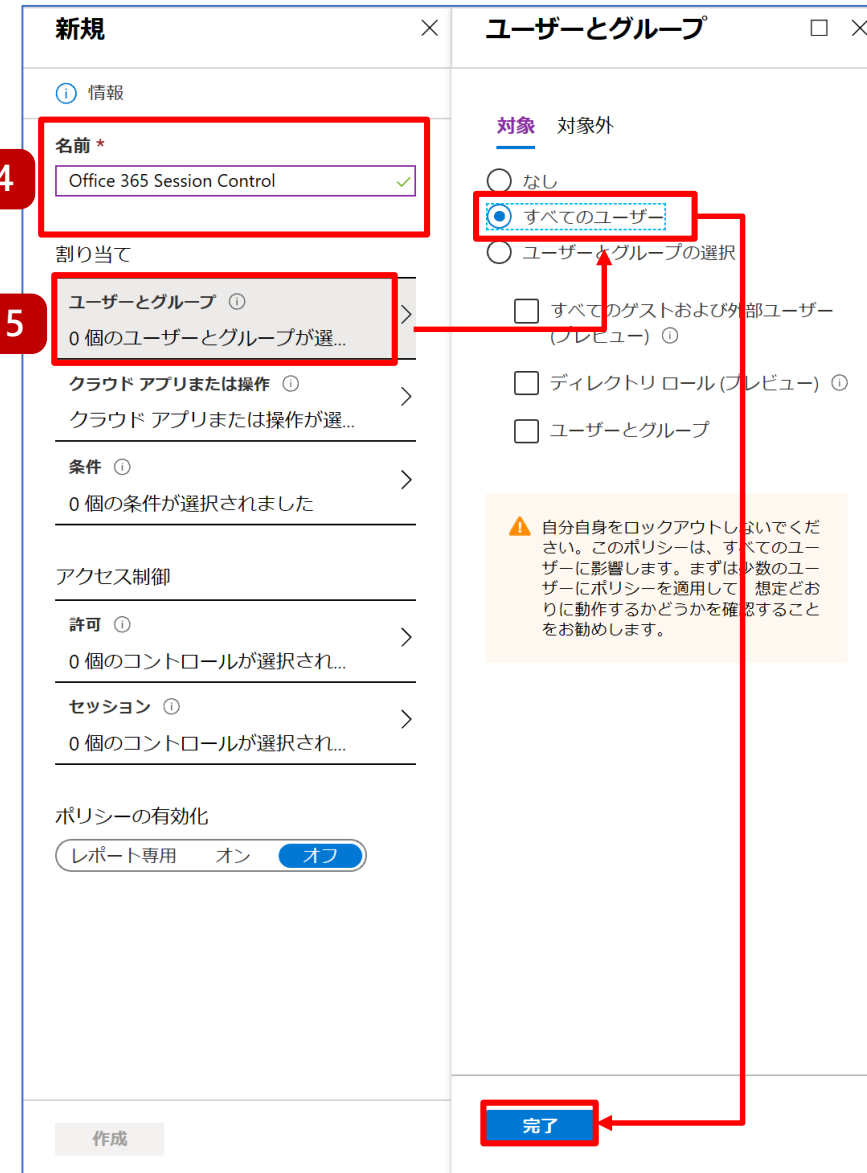
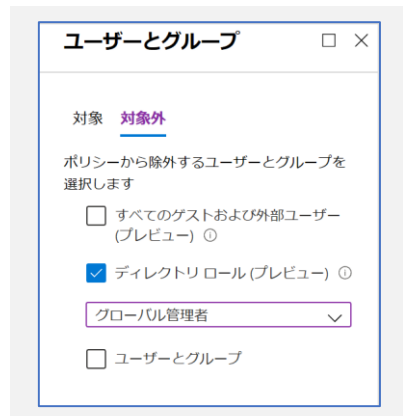


# ① Azure AD の条件付きアクセスでセッション制限を有効化

4. 新規画面で、ポリシーの名前として Office 365 Session Control と入力します。

5. 新規画面で、[ユーザーとグループ] をクリックし、[すべてのユーザー] をクリックして、[完了] をクリックします。

※状況に応じて「すべてのユーザー」ではなくポリシーを適用されたいユーザーをご指定ください。  
※「すべてのユーザー」を選択される場合は、グローバル管理者などのディレクトリロールを対象外に指定いただくことを推奨します。



新規

① 情報

名前 \*

Office 365 Session Control

割り当て

ユーザーとグループ ①

0 個のユーザーとグループが選...

クラウド アプリまたは操作 ①

クラウド アプリまたは操作が選...

条件 ①

0 個の条件が選択されました

アクセス制御

許可 ①

0 個のコントロールが選択され...

セッション ①

0 個のコントロールが選択され...

ポリシーの有効化

レポート専用 オン オフ

作成

ユーザーとグループ

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

すべてのゲストおよび外部ユーザー (プレビュー) ①

ディレクトリ ロール (プレビュー) ①

ユーザーとグループ

⚠ 自分自身をロックアウトしないでください。このポリシーは、すべてのユーザーに影響します。まずは少数のユーザーにポリシーを適用して、想定どおりに動作するかどうかを確認することをお勧めします。

完了

# ① Azure AD の条件付きアクセスでセッション制限を有効化

6. 新規画面に戻り、[クラウド アプリまたは操作] をクリックし、[アプリを選択] をクリックして、[選択] をクリックします。

7. 選択画面で、Office365 (preview) にチェックを付け、[選択] をクリックします。

※Office 365 (preview) を選択した場合は Teams、SharePoint Online、Exchange Online などの各コンポーネントが対象となります。

8. クラウド アプリまたは操作画面で、[完了] をクリックします。



# ① Azure AD の条件付きアクセスでセッション制限を有効化

9. 新規画面で、[条件] をクリックします。
10. 条件画面で、[クライアント アプリ (プレビュー)] をクリックします。
11. クライアント アプリ (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、[ブラウザー] 欄だけにチェックを付け、[完了] をクリックします。

The screenshot shows the Azure AD Conditional Access configuration process. It is divided into three main panels: '新規' (New), '条件' (Conditions), and 'クライアント アプリ (プレビュー)' (Client App Preview).

- 設定 9:** Points to the '条件' (Conditions) option in the '新規' panel, which is currently selected.
- 設定 10:** Points to the 'クライアント アプリ (プレビュー)' option in the '条件' panel.
- 設定 11:** Points to the 'はい' (Yes) radio button in the '構成' (Configure) section of the 'クライアント アプリ (プレビュー)' panel.

A summary box in the bottom right of the '条件' panel states: 「ここまでの設定で「ブラウザーから Office 365 にアクセスする場合」という条件を設定しました」 (With the settings up to this point, a condition has been set for "Accessing Office 365 from a browser").

Buttons for '作成' (Create) and '完了' (Done) are visible at the bottom of each panel.

# ① Azure AD の条件付きアクセスでセッション制限を有効化

12. 条件画面で、[デバイスの状態 (プレビュー)] をクリックします。
13. デバイスの状態 (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、[対象外] をクリックして、[ハイブリッド Azure AD 参加済み デバイス] 欄と [デバイスは準拠としてマーク済み] 欄にチェックを付け、[完了] を 2 回クリックします。

※ 社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

条件付きアクセス - ポリシー > 新規 > 条件

条件

情報

サインインのリスク 未構成

デバイス プラットフォーム 未構成

場所 未構成

デバイス プラットフォーム (プレビュー) 未構成

デバイス の状態 (プレビュー) 未構成

完了

デバイスの状態 (プレビュー)

情報

設定 13

構成

はい いいえ

対象 対象外

ポリシーからデバイスを除外するために使用するデバイスの状態の条件を選択します。

ハイブリッド Azure AD 参加済みのデバイス

デバイスは準拠としてマーク済み

完了

この設定で「会社で管理する端末以外の端末からアクセスした場合」という条件を設定しました

# ① Azure AD の条件付きアクセスでセッション制限を有効化

14. 新規画面で、[セッション] をクリックします。
15. セッション画面で、[アプリの条件付きアクセス制御を使う] 欄にチェックを付け [カスタムポリシーを使用する] を選択して [選択] をクリックします。
16. 新規画面で、[ポリシーの有効化] 欄を [オン] にし、[作成] をクリックします。

**新規**

情報

名前 \*

Office 365 Session Control **設定 15**

割り当て

ユーザーとグループ ① >  
すべてのユーザー

クラウド アプリまたは操作 ① >  
1 個のアプリ が含まれました

条件 ① >  
1 個の条件が選択されました

アクセス制御

① >  
コントロールが選択されました

セッション ① >  
0 個のコントロールが選択されました

ポリシーの有効化 **設定 16**

レポート専用 オン オフ

**セッション**

セッション制御により、クラウド アプリ内での操作の制限が可能になります。セッションの使用に関する要件を選択してください。  
[詳細情報](#)

アプリによって適用される制限を使用する ①

アプリの条件付きアクセス制御を使う ①

カスタム ポリシーを使用する... ▼

Cloud App Security ポータルでカスタム ポリシーを構成する ②  
必要があります。このコントロールは、おすすめアプリですぐに機能し、どのアプリに対してもセルフ オンボーディングが可能です。両方のシナリオの詳細については、ここをクリックしてください。

カスタム ポリシーの構成

サインインの頻度 ①

永続的なブラウザ セッション ①

この設定で「Cloud App Security で設定したポリシーに基づいてアクセスを制御します」という設定をしました

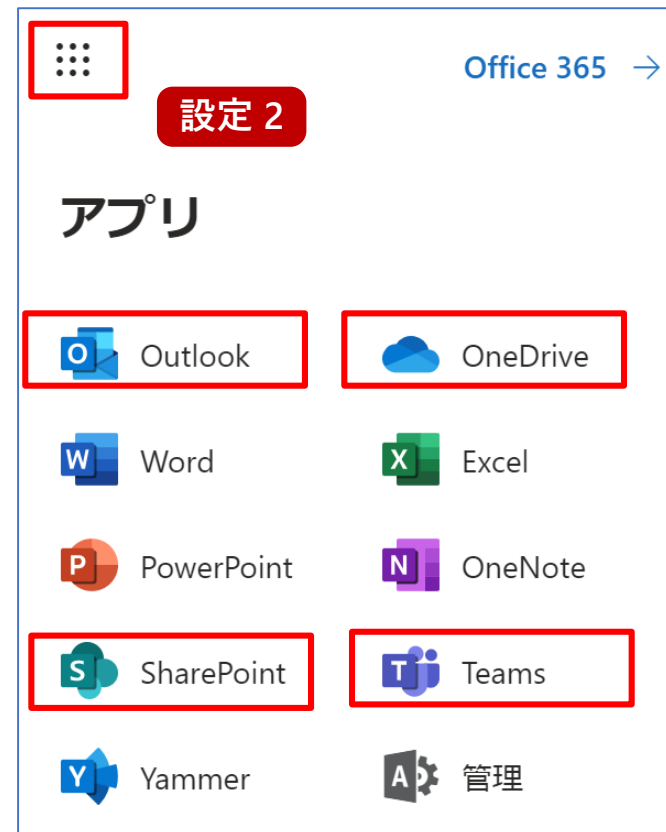
**選択**

## ② Microsoft Cloud App Security でセッション制御の有効化を確認

1. ブラウザー画面を開き、Exchange Online の URL <https://outlook.office365.com> にアクセスします。

※前項の手順で作成した Azure AD のポリシーの適用対象のユーザーにて実施します。

2. 画面左上のボタンをクリックし、  
[SharePoint] や [Exchange Online]  
[Teams] [OneDrive] などを  
クリックします。



## ② Microsoft Cloud App Security でセッション制御の有効化を確認

3. ブラウザー画面を開き、Cloud App Security 管理ポータル URL <https://portal.cloudappsecurity.com> にアクセスします。

4. Cloud App Security 管理ポータル画面で、[調査] - [接続アプリ] をクリックし、[アプリの条件付きアクセス制御アプリ] をクリックして、Office 365 の各コンポーネントが表示されていることを確認します。

The screenshot shows the 'Cloud App Security' management portal. The left sidebar contains a menu with '調査' (Investigation) selected. Below it, '接続アプリ (2)' (Connected Applications (2)) is highlighted. A red box labeled '設定 4' (Setting 4) points to the '接続アプリ (2)' menu item. Another red box labeled 'アプリの条件付きアクセス制御 アプリ' (Conditional Access Control Applications) points to the corresponding application in the main content area. The main content area shows a table of applications with columns for '状態' (Status), '利用可能な制御' (Available Controls), '接続日時' (Connection Date/Time), and '最後のアクティビティ' (Last Activity).

状態	利用可能な制御	接続日時	最後のアクティビティ
接続済み	Azure AD 条件付きアクセス制御	2020年2月18日, 14:56	
接続済み	Azure AD 条件付きアクセス制御	2020年2月18日, 14:56	
接続済み	Azure AD 条件付きアクセス制御	2020年3月23日, 19:02	

### ③ Microsoft Cloud App Security でセッションポリシーを設定

1. Cloud App Security 管理ポータル画面で、左上のボタンをクリックし、[制御] - [ポリシー] をクリックします。
2. ポリシー画面で、[ポリシーの作成] - [セッションポリシー] をクリックします。





### ③ Microsoft Cloud App Security でセッションポリシーを設定

3. セッションポリシーの作成画面で、[ポリシー テンプレート] 欄から [リアルタイムのコンテンツ検査に基づいてダウンロードをブロックします] を選択します。
4. テンプレートを適用しますか？画面で、[テンプレートの適用] をクリックします。



### ③ Microsoft Cloud App Security でセッションポリシーを設定

5. セッションポリシーの作成画面で、下にスクロールし、[検査方法] 欄から [なし] を選択して、[作成] をクリックします。

Cloud App Security

ポリシーへのファイルフィルターの追加

次のすべてに一致するファイル

フィルターの選択...

検査方法

なし

設定 5

アクション

ユーザー アクティビティがポリシーに一致した場合に適用されるアクションを選んでください。

テスト  
すべてのアクティビティを監視する

ブロック  
ファイルのダウンロードをブロックし、すべてのアクティビティを監視します

ユーザーにメールでも通知する

ブロックメッセージのカスタマイズ

保護  
ダウンロードしたファイルに分類ラベルを適用し、すべてのアクティビティを監視します

一致するイベントごとにポリシー重要度に応じたアラートを作成する 既定の設定に戻す

日次アラート制限 5

アラートをメールで送信

アラートをテキストメッセージとして送信する

既定の設定として保存

Power Automate にアラートを送信する  
Power Automate でブレイックを作成する

ここまでの操作で「非管理 PC からのブラウザを利用した Office 365 アクセスを許可するが、ファイルのダウンロードをブロックする」という設定をしました

### ③ Microsoft Cloud App Security でセッションポリシーを設定

6. ポリシー画面で、[ポリシーの作成] - [セッション ポリシー] をクリックします。
7. セッション ポリシーの作成画面で、[ポリシー テンプレート] 欄から [リアルタイムのコンテンツ検査に基づいて切り取り、コピー、貼り付けをブロックします] を選択します。
8. テンプレートを適用しますか？画面で、[テンプレートの適用] をクリックします。



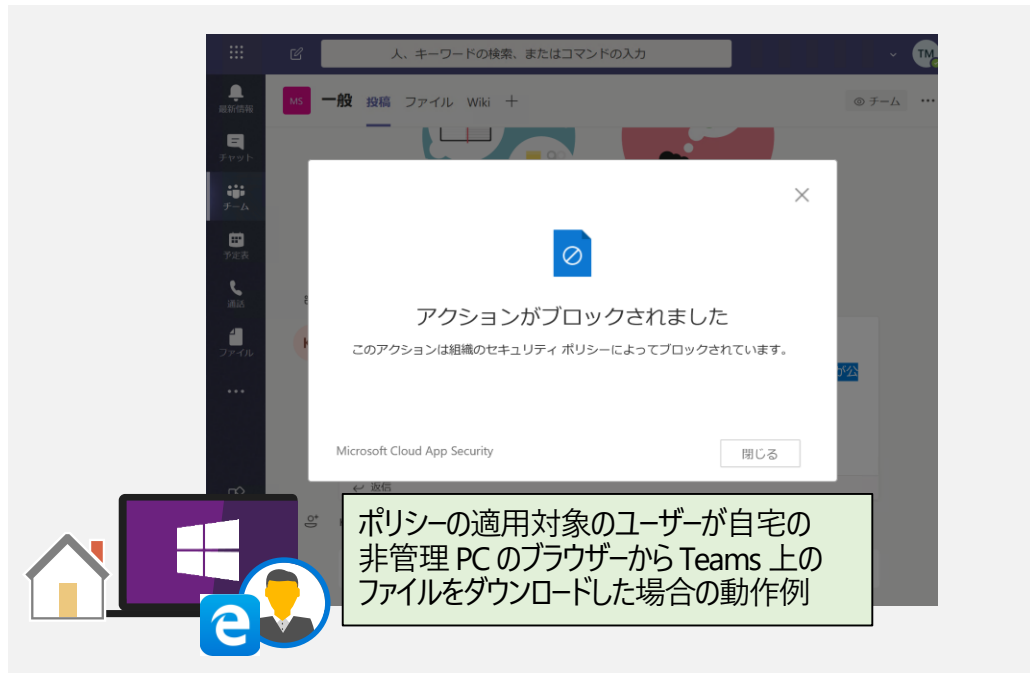
### ③ Microsoft Cloud App Security でセッションポリシーを設定

9. セッションポリシーの作成画面で、[アクティビティソース] 欄の [Print Cut/Copy item, Paste item] 項目をクリックして、[Print], [Cut/Copy item], [Paste item] にチェックが付くようにクリックします。



### ③ Microsoft Cloud App Security でセッションポリシーを設定

10. セッションポリシーの作成画面で、[コンテンツ検査] 欄の [有効] 項目からチェックを外します。
11. セッションポリシーの作成画面で、[作成] をクリックします。



### ③ Microsoft Cloud App Security でセッションポリシーを設定

12. セッション ポリシーの作成画面で、[ポリシー テンプレート] 欄から [リアルタイムのコンテンツ検査に基づいてアップロードをブロックします] を選択します。
13. テンプレートを適用しますか？画面で、[テンプレートの適用] をクリックします。

Cloud App Security

#### セッション ポリシーの作成

セッションポリシーにより、リアルタイム監視と、クラウド アプリのユーザー アクティビティの制御が可能になります。

ポリシー テンプレート  
リアルタイムのコンテンツ検査に基づいてアップロードをブロック... **設定 12**

ポリシー名  
リアルタイムのコンテンツ検査に基づいてアップロードをブロックし

説明  
Cloud App Security は、アップロードしているファイルの内容をリアルタイムで評価し、違反内容をブロックします。

ポリシー重要度  
中

カテゴリ  
DLP

セッション制御の種類  
有効にするコントロールの種類を選択してください  
ファイル アップロードの制御 (DLP 使用)

アクティビティ ソース  
ポリシーにアクティビティ フィルターを追加する

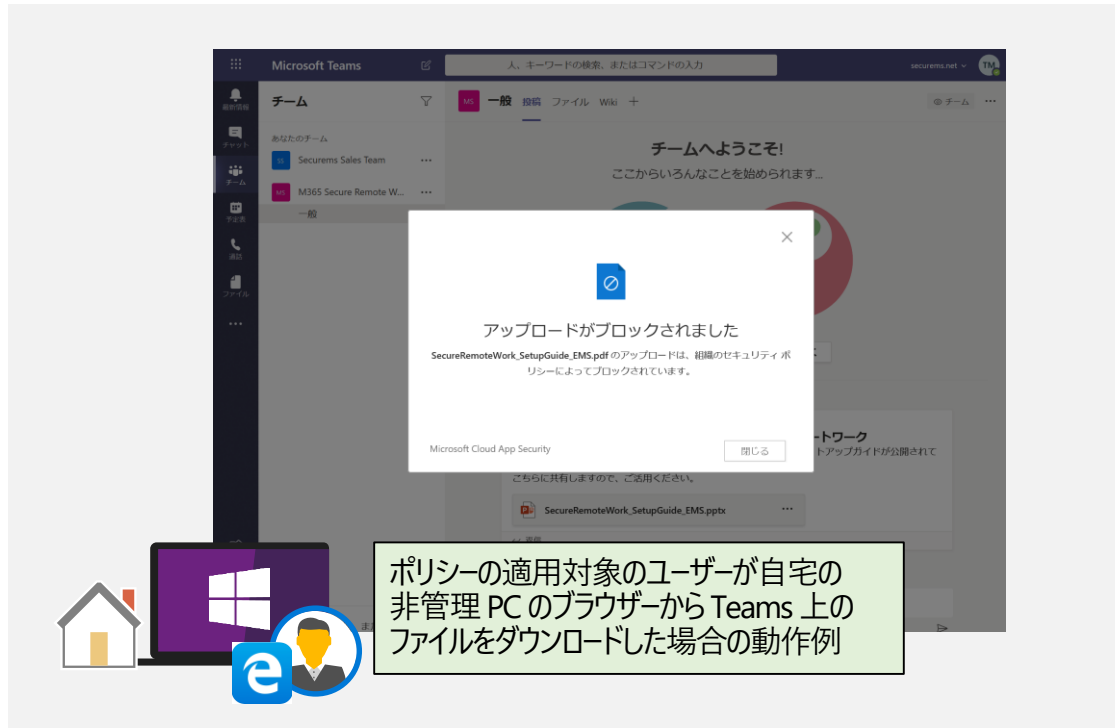
次のすべてに一致する アクティビティ 結果の編集とプレビュー

- × デバイス タグ が次に等しくない
- 準拠している、ドメイ...

+

### ③ Microsoft Cloud App Security でセッションポリシーを設定

14. セッションポリシーの作成画面で、下にスクロールし、[検査方法] 欄から [なし] を選択して、[作成] をクリックします。

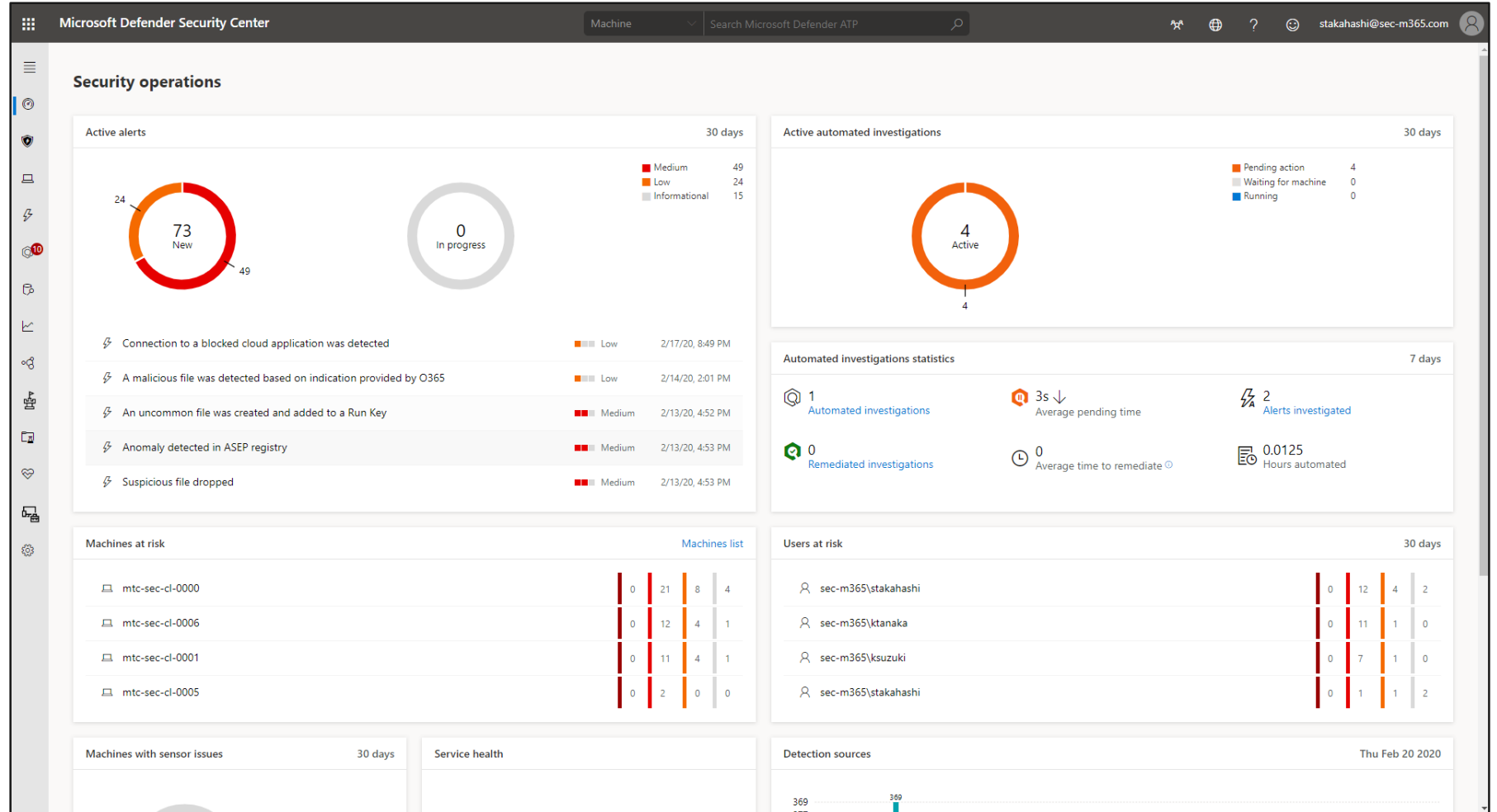


# ④ Microsoft Defender Security Center へのサインイン

## 必要な権限

- Global Administrator
- Security Administrator
- Security Reader

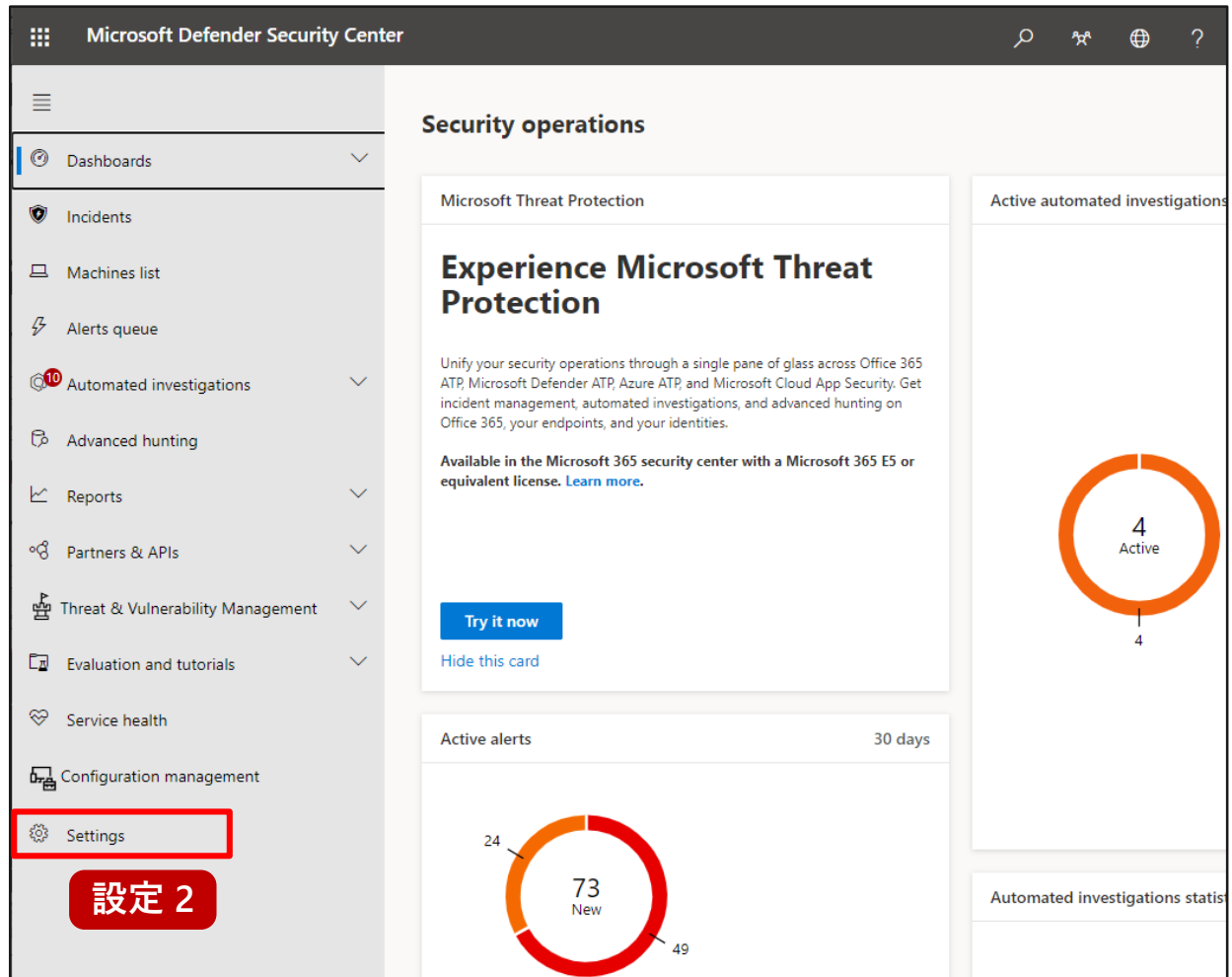
<https://securitycenter.windows.com/>





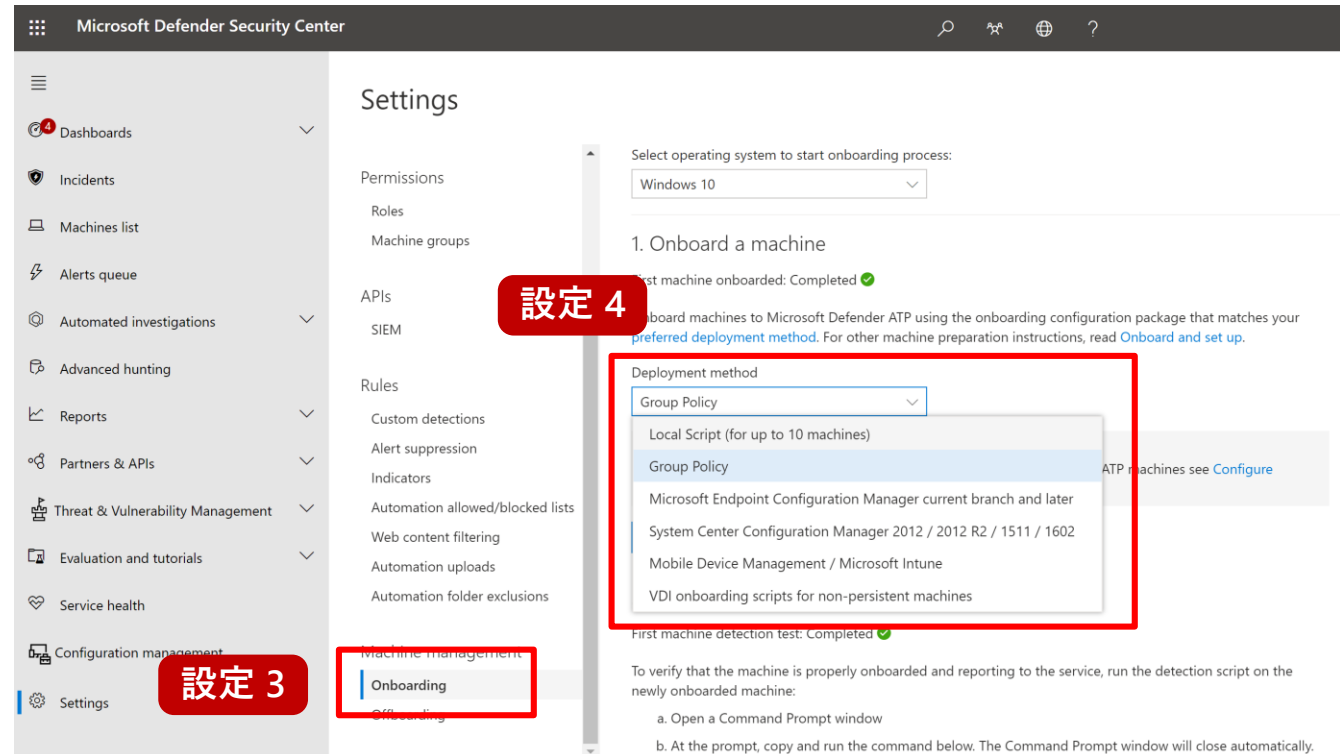
## ④ Microsoft Defender ATP 登録手順

1. ブラウザー画面を開き、Microsoft Defender ATP の URL <https://securitycenter.windows.com/> にアクセスします。
2. Windows Defender Security Center 画面で、[Settings] をクリックします。



## ④ Microsoft Defender ATP 登録手順

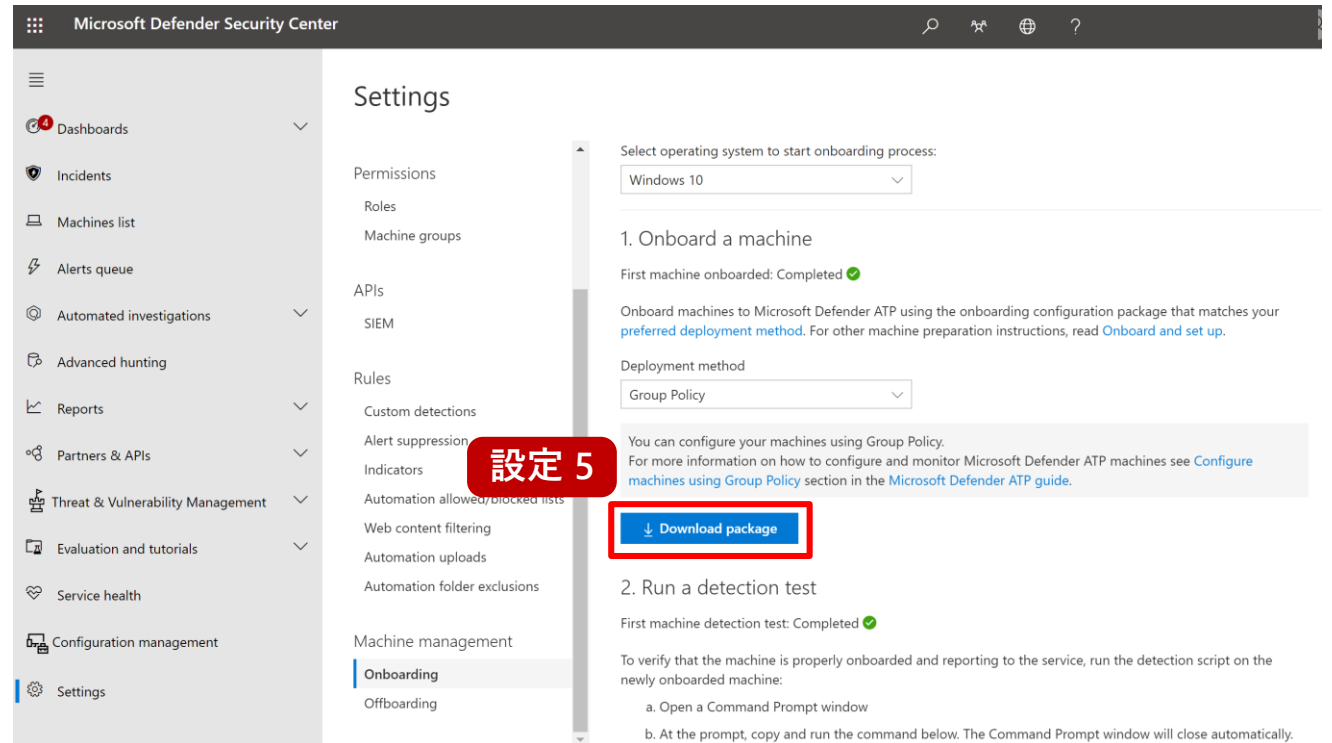
3. Settings 画面で、[Onboarding] をクリックします。
4. Settings 画面で、[Deployment method] 欄から [Group Policy] を選択します。



The screenshot shows the Microsoft Defender Security Center interface. The left sidebar contains navigation options like Dashboards, Incidents, Machines list, Alerts queue, Automated investigations, Advanced hunting, Reports, Partners & APIs, Threat & Vulnerability Management, Evaluation and tutorials, Service health, and Configuration management. The main content area is titled 'Settings' and includes sections for Permissions, APIs, Rules, and Machine management. The 'Onboarding' option under Machine management is highlighted with a red box and labeled '設定 3'. The 'Deployment method' dropdown menu is open, showing options: Group Policy (selected), Local Script (for up to 10 machines), Group Policy, Microsoft Endpoint Configuration Manager current branch and later, System Center Configuration Manager 2012 / 2012 R2 / 1511 / 1602, Mobile Device Management / Microsoft Intune, and VDI onboarding scripts for non-persistent machines. This dropdown menu is also highlighted with a red box and labeled '設定 4'. The main content area displays instructions for onboarding a machine, including a dropdown for 'Select operating system to start onboarding process:' set to 'Windows 10', and a section titled '1. Onboard a machine' with a 'Deploy machine onboarding: Completed' status. Below this, it says 'Onboard machines to Microsoft Defender ATP using the onboarding configuration package that matches your preferred deployment method. For other machine preparation instructions, read Onboard and set up.' The 'First machine detection test: Completed' status is also visible.

## ④ Microsoft Defender ATP 登録手順

5. Settings 画面で、[Download package] をクリックして、スクリプトをダウンロードします。



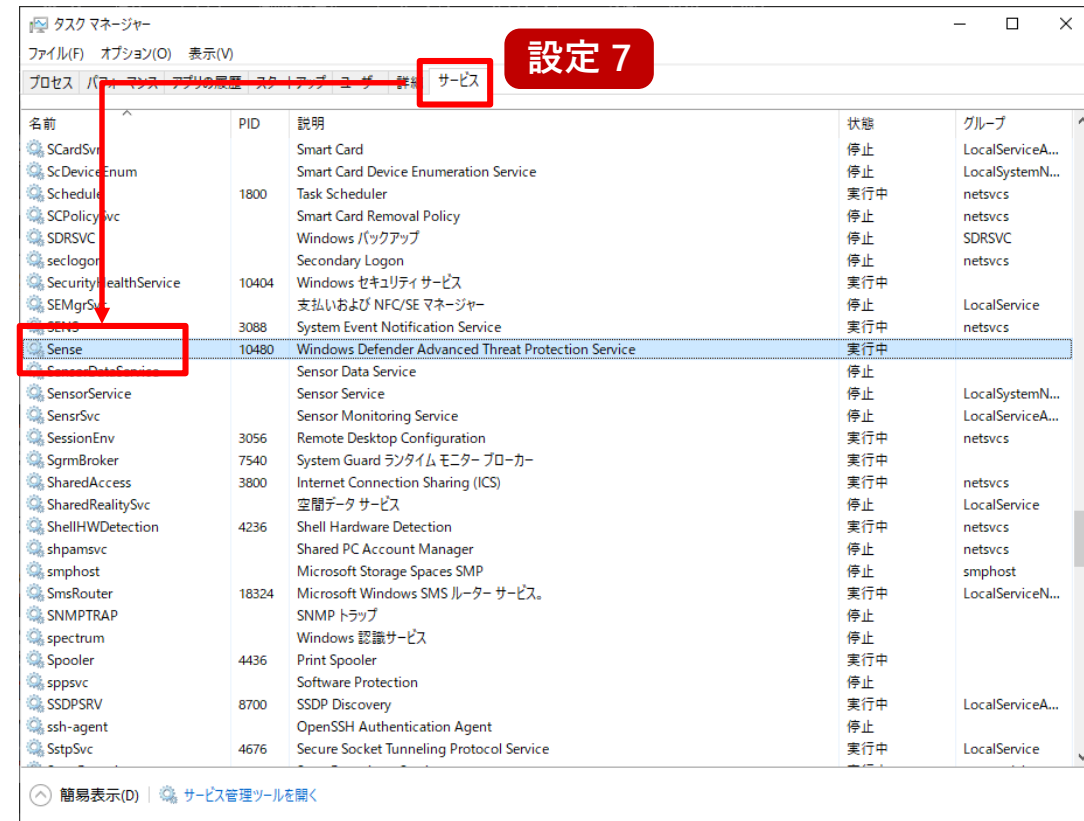
The screenshot shows the Microsoft Defender Security Center interface. The left sidebar contains navigation options, with 'Settings' selected at the bottom. The main content area is titled 'Settings' and includes a list of categories on the left: Permissions, Roles, Machine groups, APIs, SIEM, Rules, Custom detections, Alert suppression, Indicators, Automation allowed/blocked lists, Web content filtering, Automation uploads, Automation folder exclusions, Machine management, Onboarding, and Offboarding. The 'Onboarding' category is currently selected. The right pane displays the 'Onboard a machine' section, which includes a dropdown for 'Select operating system to start onboarding process:' set to 'Windows 10', a 'Deployment method' dropdown set to 'Group Policy', and a 'Download package' button. A red callout box with the text '設定 5' (Setting 5) points to the 'Download package' button. Below the button, there are instructions for running a detection test.

## ④ Microsoft Defender ATP 登録手順

6. ダウンロードしたファイルを Windows 10 デバイスで実行します。すると、Microsoft Defender ATP にデバイスが登録されます。



7. デバイス上で登録ができたことはタスクマネージャー (Ctrl + Shift + Esc キー) から [サービス] タブをクリックして、Sense サービスが登録されていることで確認できます。



# 最小構成プラン 編

※本ガイドの P.30-59 の手順が対象となります。

---

## Enterprise Mobility + Security E3

- Azure Active Directory Premium P1
- Microsoft Intune



# 設定手順

- ① SharePoint Online のアクセスポリシーを有効化する
- ② Exchange Online のアクセスポリシーを有効化する
- ③ Azure AD の条件付きアクセスで上記 2 つのポリシーを展開する

※セッション制御の対象はブラウザ利用時のみとなります。非管理 PC の Office アプリからのアクセスをブロックしたい場合は後述の P.52 以降をご参照ください。

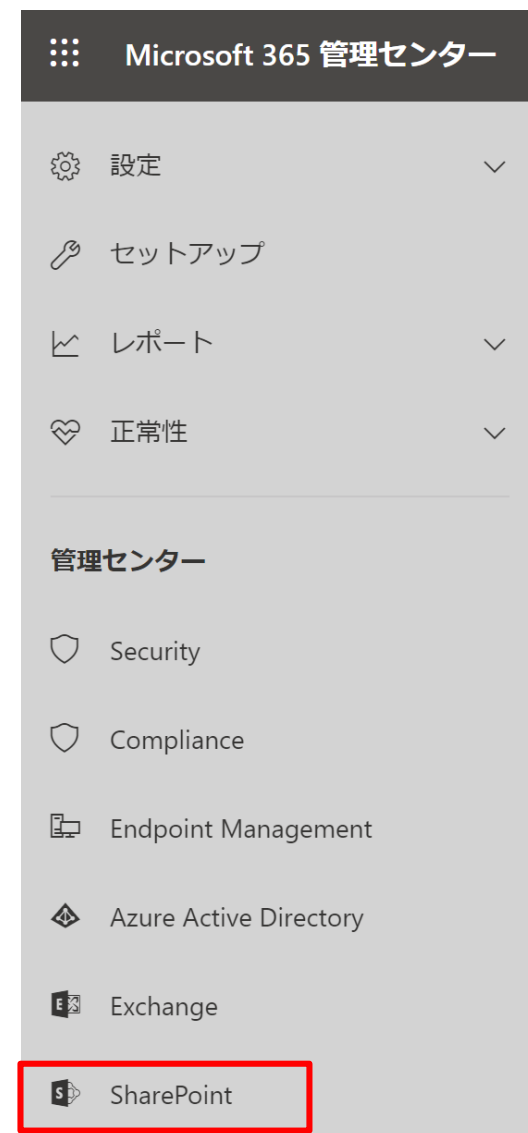
※ 社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

## ① SharePoint Online のアクセスポリシーを有効化する

1. ブラウザー画面を開き、Azure Active Directory 管理センターの URL

<http://portal.microsoft.com/adminportal>  
にアクセスします。

2. Microsoft 365 管理センター画面で、[SharePoint] をクリックします。



# ① SharePoint Online のアクセスポリシーを有効化する

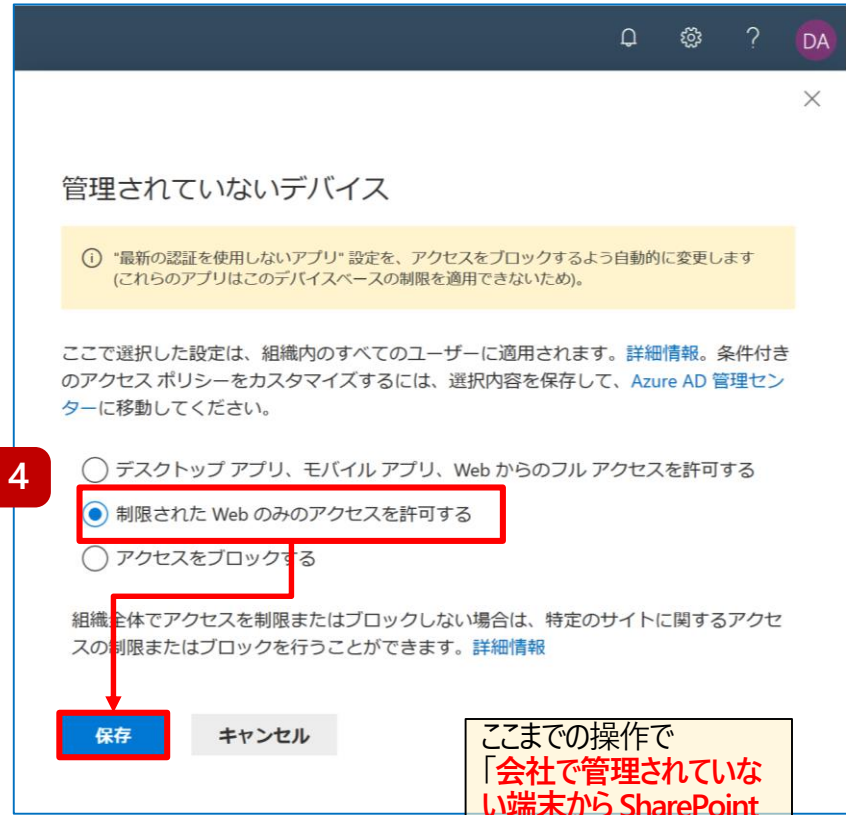
3. SharePoint 管理センター画面で [ポリシー] - [アクセスの制御] をクリックし、[管理されていないデバイス] をクリックします。





# ① SharePoint Online のアクセスポリシーを有効化する

4. 管理されていないデバイス画面で [制限された Web のみのアクセスを許可する] を選択し、[保存] をクリックします。



**重要！**

SharePoint の本設定を有効化すると Azure AD 上の条件付きアクセスに以下の 2 つのポリシーが自動で ON の状態で作成されます。必ず設定を OFF に変更ください。

[SharePoint admin center]Block access from apps on unmanaged devices - 2

[SharePoint admin center]Use app-enforced Restrictions for browser access

ここまでの操作で「会社で管理されていない端末から SharePoint Online へのアクセスには特定の操作だけができるようにする」という設定をしました

## ② Exchange Online のアクセスポリシーを有効化

1. スタートボタンを右クリックし、[Windows PowerShell (管理者)] をクリックします。
2. Windows PowerShell 画面で、次のコマンドレットを実行します。

1.	<code>Set-ExecutionPolicy RemoteSigned</code>
2.	<code>\$UserCredential = Get-Credential</code>

## ② Exchange Online のアクセスポリシーを有効化

3. サインイン画面で、管理者のユーザー名とパスワードを入力し、サインインします。
4. Windows PowerShell 画面で、次のコマンドレットを実行します。

```
3. $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri  
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential  
-Authentication Basic -AllowRedirection  
4. Import-PSSession $Session -DisableNameChecking  
5. Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
```

ここまでの操作で  
「会社で管理されていない端末から Exchange Online へのアクセスには特定の操作だけができるようにする」  
という設定をしました

### ③ Azure AD の条件付きアクセスでポリシーを展開

1. ブラウザー画面を開き、Azure Active Directory 管理センターの URL <https://aad.portal.azure.com> にアクセスします。
2. Azure Active Directory 管理センター画面で、[Azure Active Directory] - [セキュリティ] - [条件付きアクセス] の順にクリックします。
3. 条件付きアクセス画面で、[新しいポリシー] をクリックします。

### ③ Azure AD の条件付きアクセスでポリシーを展開

4. 新規画面で、ポリシーの名前として ExO/SPO Session Control と入力します。

5. 新規画面で、[ユーザーとグループ] をクリックし、[すべてのユーザー] をクリックして、[完了] をクリックします。

※状況に応じて「すべてのユーザー」ではなくポリシーを適用されたいユーザーをご指定ください。  
※「すべてのユーザー」を選択される場合は、全体管理者などのディレクトリロールを対象外に指定いただくことを推奨します。

新規

ユーザーとグループ

情報

名前 \*

ExO/SPO Session Control

割り当て

ユーザーとグループ ①

0 個のユーザーとグループが選択さ...

クラウド アプリまたは操作 ①

クラウド アプリまたは操作が選択さ...

条件 ①

0 個の条件が選択されました

アクセス制御

許可 ①

0 個のコントロールが選択されました

セッション ①

0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 オン オフ

作成

完了

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

すべてのゲストおよび外部ユーザー (プレビュー) ①

ディレクトリロール (プレビュー) ①

ユーザーとグループ

自分自身をロックアウトしないでください。このポリシーは、すべてのユーザーに影響します。まずは少数のユーザーにポリシーを適用して、想定どおりに動作するかどうかを確認することをお勧めします。

ユーザーとグループ

対象 対象外

ポリシーから除外するユーザーとグループを選択します

すべてのゲストおよび外部ユーザー (プレビュー) ①

ディレクトリロール (プレビュー) ①

グローバル管理者

ユーザーとグループ

### ③ Azure AD の条件付きアクセスでポリシーを展開

6. 新規画面に戻り、[クラウド アプリまたは操作] をクリックし、[アプリを選択] をクリックして、[選択] をクリックします。

7. 選択画面で、Office365 Exchange Online と SharePoint Online にチェックを付け、[選択] をクリックします。

8. クラウド アプリまたは操作画面で、[完了] をクリックします。

新規

クラウド アプリまたは操作

このポリシーが適用される対象を選択する

クラウド アプリ ユーザー操作

対象 対象外

なし

すべてのクラウド アプリ

アプリを選択

選択

Office 365 SharePoint Online、...

Office 365 Exchange O... ..

Office 365 SharePoint ... ..

選択したアプリのうち少なくとも 1 つは Office 365 の一部です。代わりに、Office 365 アプリでポリシーを設定することをお勧めします。

SharePoint Online を選択すると、Microsoft Teams、Planner、Delve、MyAnalytics、Newsfeed などのアプリにも適用されます。

設定 6

設定 7

設定 8

完了

### ③ Azure AD の条件付きアクセスでポリシーを展開

9. 新規画面で、[条件] をクリックします。
10. 条件画面で、[クライアント アプリ (プレビュー)] をクリックします。
11. クライアント アプリ (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、[ブラウザー] 欄だけにチェックを付け、[完了] をクリックします。

The screenshot shows the Azure AD Conditional Access configuration interface. It is divided into three main panels:

- 新規 (New):** Shows the '名前' (Name) field set to 'ExO/SPO Session Control'. Under '割り当て' (Assign to), 'ユーザーとグループ' (Users and groups) is set to 'すべてのユーザー' (All users). Under 'アクセス制御' (Access control), '許可' (Permissions) and 'セッション' (Sessions) are both set to '0個のコントロールが選択されました' (0 controls selected). The 'ポリシーの有効化' (Policy activation) is set to 'オフ' (Off). A red box labeled '設定 9' highlights the '条件' (Conditions) link.
- 条件 (Conditions):** Shows a list of conditions. 'クライアント アプリ (プレビュー)' (Client app (preview)) is highlighted with a red box labeled '設定 10'. A red arrow points from this box to the 'クライアント アプリ (プレビュー)' panel.
- クライアント アプリ (プレビュー) (Client app (preview)):** Shows the '構成' (Configure) section with the 'はい' (Yes) radio button selected. Under 'このポリシーを適用するクライアント アプリを選択します' (Select client apps to which this policy applies), the 'ブラウザー' (Browser) checkbox is checked. A red box labeled '設定 11' highlights the 'はい' button. A red arrow points from this box to the '完了' (Done) button at the bottom.

A yellow callout box at the bottom of the '条件' panel contains the text: 'ここまでの設定で「ブラウザーから Exchange Online または SharePoint Online にアクセスする場合」という条件を設定しました' (With the settings up to this point, the condition 'Access from browser to Exchange Online or SharePoint Online' has been set).

### ③ Azure AD の条件付きアクセスでポリシーを展開

12. 条件画面で、[デバイスの状態 (プレビュー)] をクリックします。
13. デバイスの状態 (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、[対象外] をクリックして、[ハイブリッド Azure AD 参加済みデバイス] 欄と [デバイスは準拠としてマーク済み] 欄にチェックを付け、[完了] を 2 回クリックします。

※ 社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

この設定で「会社で管理する端末以外の端末からアクセスした場合」という条件を設定しました



### ③ Azure AD の条件付きアクセスでポリシーを展開

14. 新規画面で、[セッション] をクリックします。
15. セッション画面で、[アプリによって適用される制限を使用する] 欄にチェックをつけて [選択] をクリックします。
16. 新規画面で、[ポリシーの有効化] 欄を [オン] にし、[作成] をクリックします。

新規

セッション

セッション制御により、クラウド アプリ内での操作の制限が可能になります。この使用に関する要件を選択してください。

**設定 15**

アプリによって適用される制限を使用する ①

アプリの条件付きアクセス制御を使う ①

サインインの頻度 (プレビュー) ①

永続的なブラウザー セッション (プレビュー) ①

**設定 14**

セッション ①  
0 個のコントロールが選択されました

ポリシーの有効化  
レポート専用 **オン** オフ

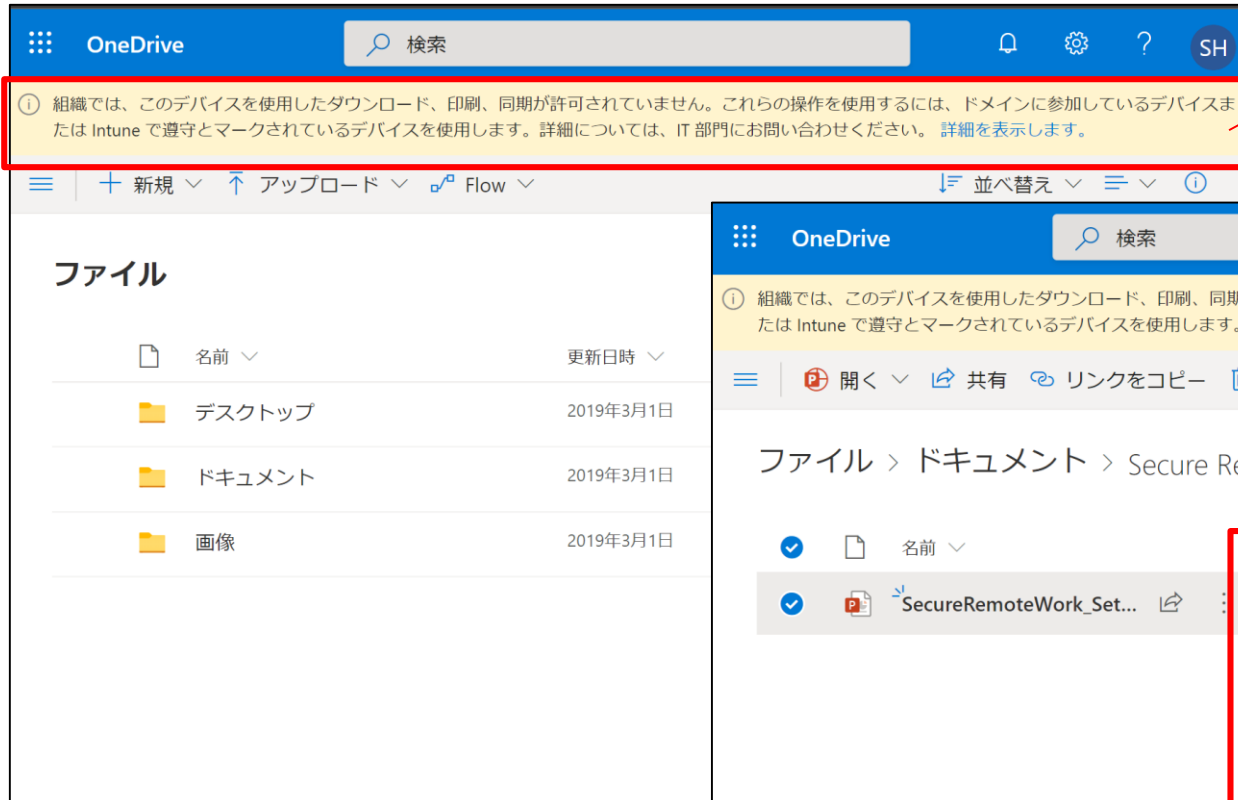
**設定 16**

作成

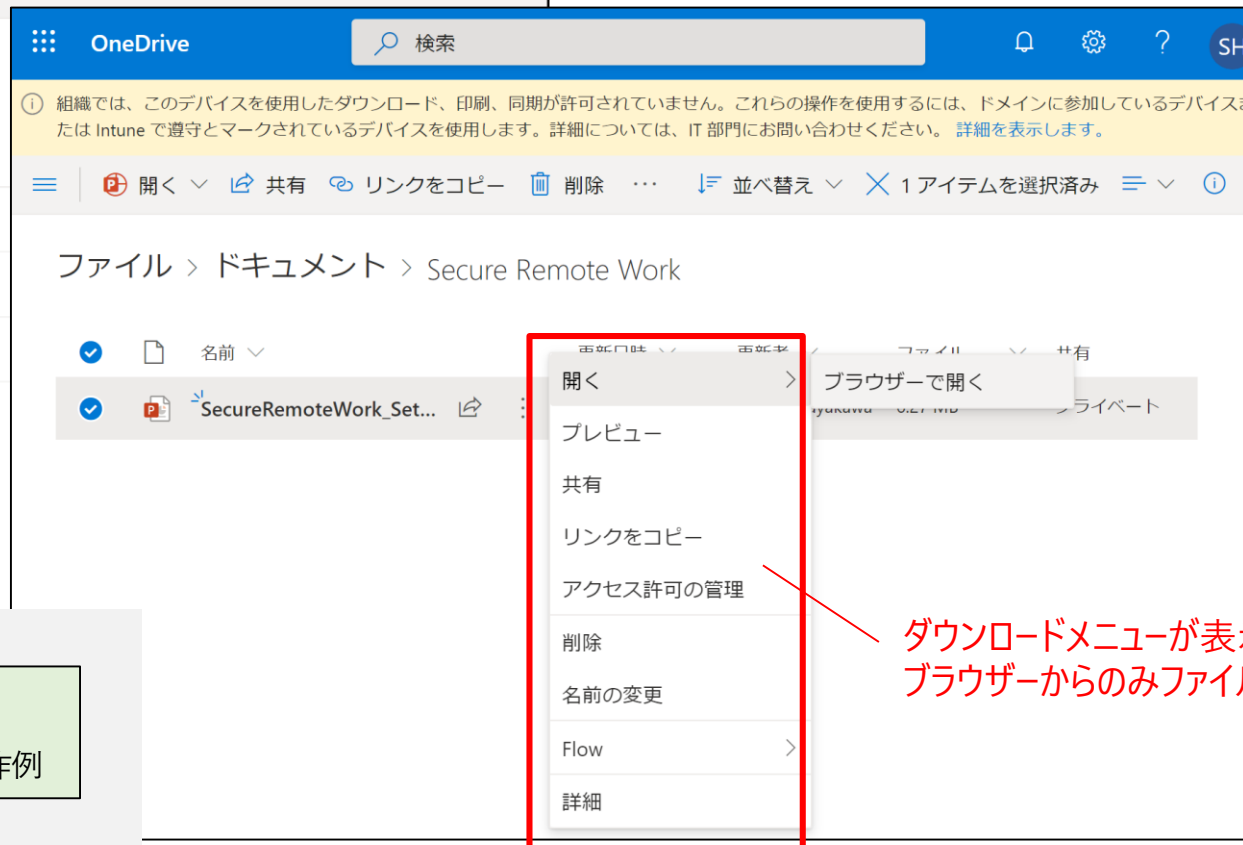
選択

ここまでの設定で「Exchange Online と SharePoint Online で設定した内容に基づいてアクセスを制限します」という設定をしました

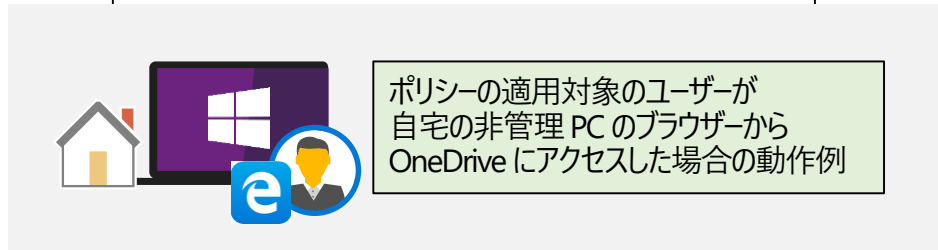
### ③ Azure AD の条件付きアクセスでポリシーを展開



非管理 PC からのアクセスであるため、一部操作が制限される旨のメッセージを表示



ダウンロードメニューが表示されず、ブラウザからのみファイルを開くことが可能



# Appendix1 : 両プラン共通の推奨設定

---

- レガシ認証のブロック
- 非管理 PC の Office アプリからの Office 365 アクセスのブロック
- Azure AD の条件付きアクセスの社内ネットワーク利用時の除外設定

# 設定手順

① Azure AD の条件付きアクセスでレガシ認証をブロックするポリシーを展開する

※ 社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

② Azure AD の条件付きアクセスで非管理 PC の Office クライアントアプリからの Office 365 アクセスをブロックするポリシーを展開する

※ 社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

③ Azure AD の条件付きアクセスの社内ネットワーク利用時の除外設定

# レガシ認証とは

レガシ認証とは、基本認証を使用するプロトコルのことです。通常、これらのプロトコルでは、第 2 要素の認証 (多要素認証) を適用できません。レガシ認証に基づくアプリの例を下記に示します。

- 従来の Microsoft Office アプリ (Modern Authentication 非対応 Office アプリ)
- POP、IMAP、SMTP などの電子メール プロトコルを使用するアプリ

上記は単 1 要素認証 (例：ユーザー名/パスワード) のみが利用可能であり、第 2 要素の認証 (多要素認証) を適用できません。これらのプロトコルの利用時は悪意のある第三者からの資格情報に対する攻撃に対して十分なセキュリティを確保することが出来ないことから、これらのプロトコルの利用を Azure AD 上でブロックすることが推奨されます。

本ガイドでは、Azure AD の条件付きアクセスを利用したレガシ認証をブロックするための構成例を記載しています。詳細については下記の URL もご参考ください。

**条件付きアクセスを使用して Azure AD へのレガシ認証をブロックする**

<https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/block-legacy-authentication>

## ① レガシ認証のブロック

1. ブラウザー画面を開き、Azure Active Directory 管理センターの URL <https://aad.portal.azure.com> にアクセスします。
2. Azure Active Directory 管理センター画面で、[Azure Active Directory] - [セキュリティ] - [条件付きアクセス] の順にクリックします。
3. 条件付きアクセス画面で、[新しいポリシー] をクリックします。

# ① レガシ認証のブロック

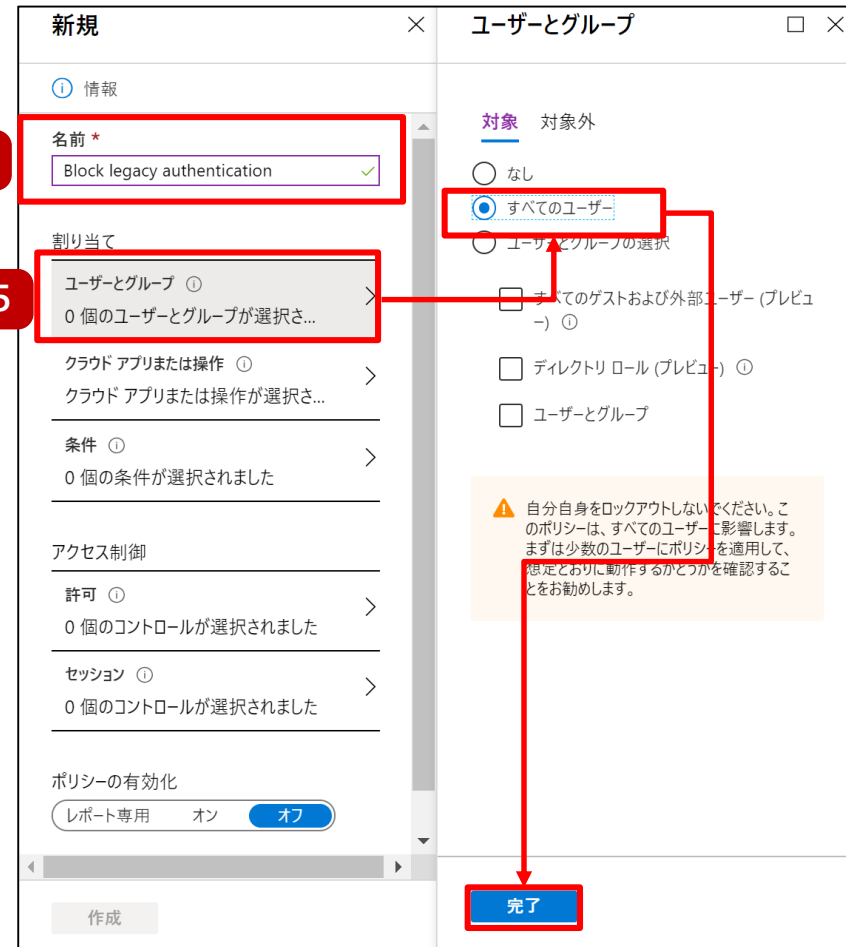
4. 新規画面で、ポリシーの名前として Block legacy authentication と入力します。

5. 新規画面で、[ユーザーとグループ] をクリックし、[すべてのユーザー] をクリックして、[完了] をクリックします。

※状況に応じて「すべてのユーザー」ではなくポリシーを適用されたいユーザーをご指定ください。

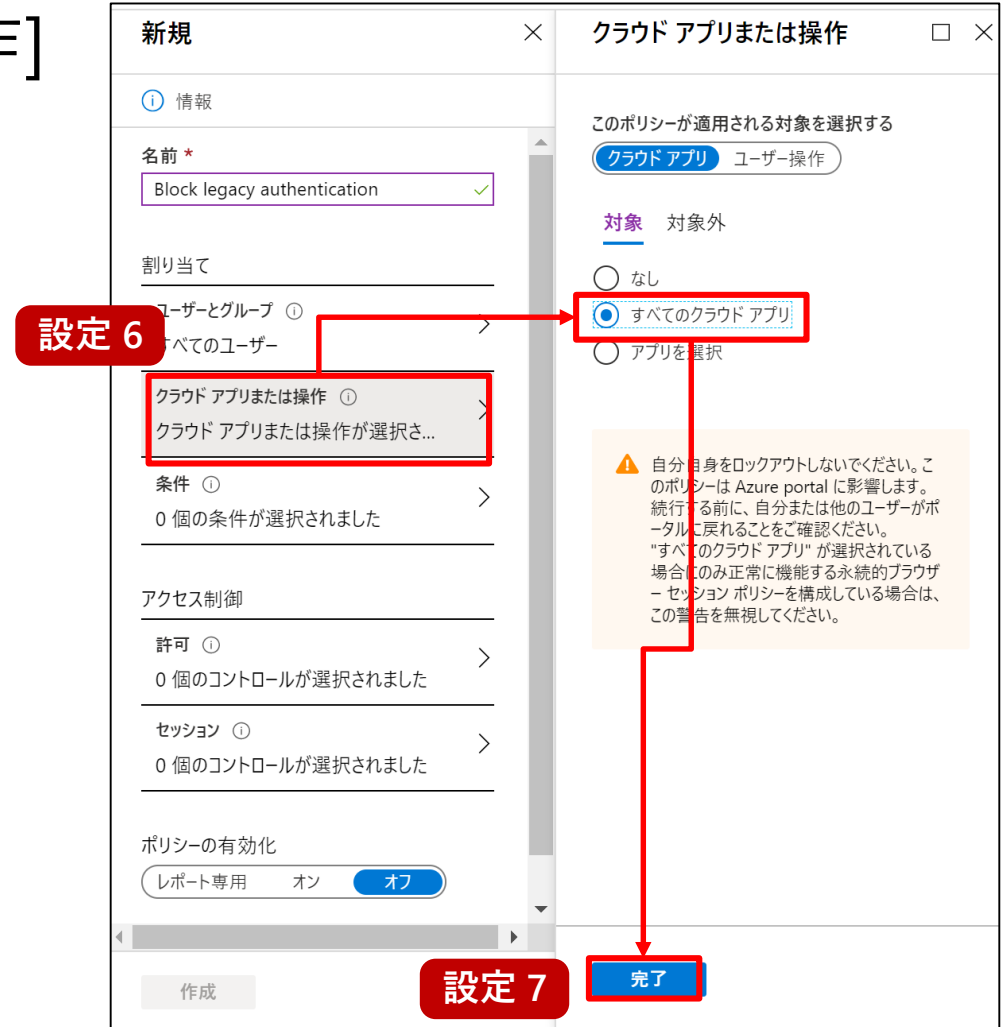
設定 4

設定 5



# ① レガシ認証のブロック

6. 新規画面に戻り、[クラウド アプリまたは操作] をクリックし、[すべてのクラウドアプリ] を選択します。
7. クラウド アプリまたは操作画面で、[完了] をクリックします。



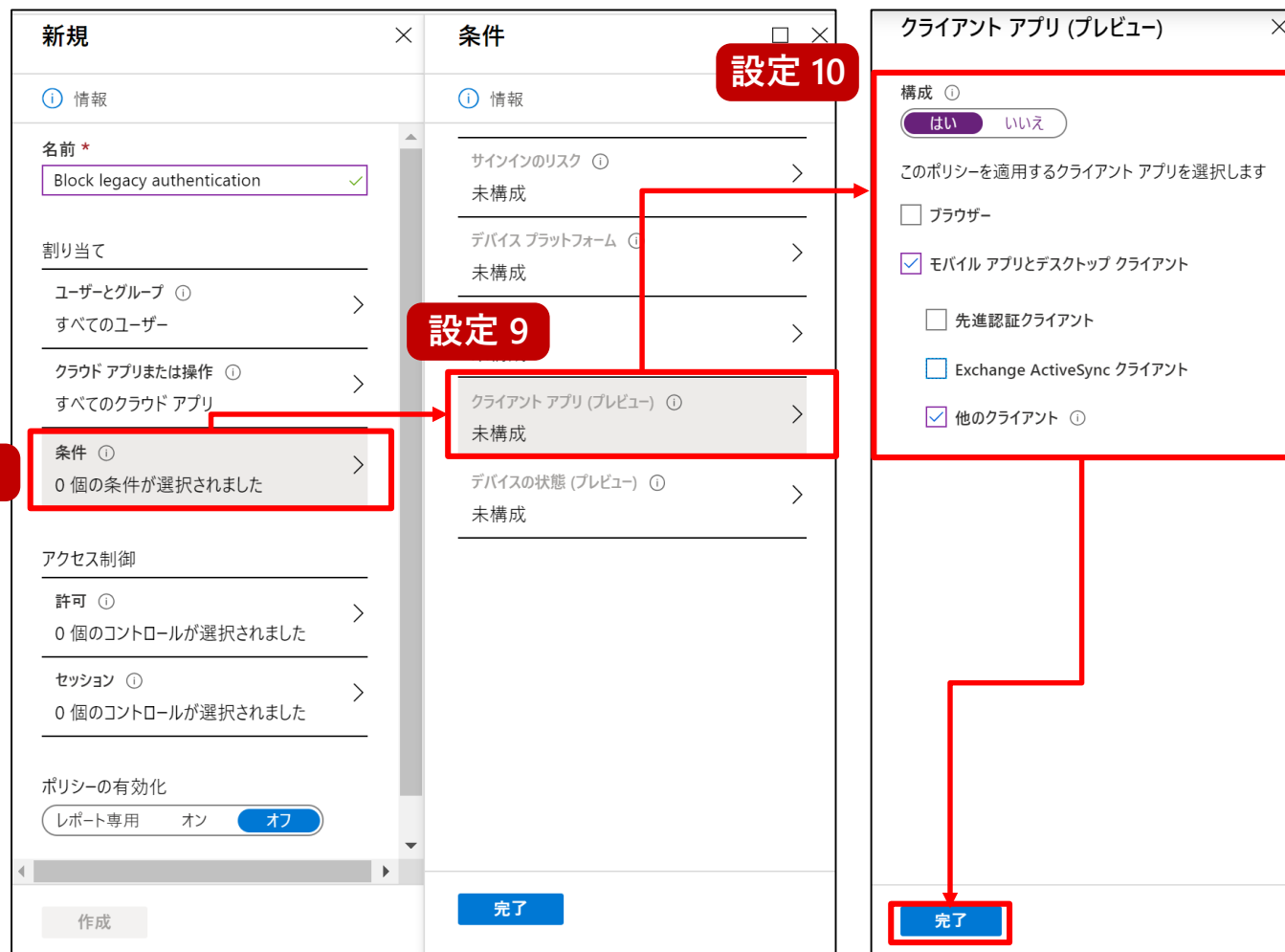


# ① レガシ認証のブロック

8. 新規画面で、[条件] をクリックします。

9. 条件画面で、[クライアント アプリ (プレビュー)] をクリックします。

10. クライアント アプリ (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、[他のクライアント] 欄だけにチェックを付け、[完了] をクリックします。



# ① レガシ認証のブロック

11. 新規画面で、[許可] をクリックします。

12. 許可の画面で、[アクセスのブロック] をクリックし、[選択]をクリックします。

13. 新規画面で、[ポリシーの有効化] 欄を[オン] にし、[作成] をクリックします。

新規

情報

名前 \*  
Block legacy authentication ✓

割り当て

ユーザーとグループ ① >  
すべてのユーザー

クラウド アプリまたは操作 ① >  
すべてのクラウド アプリ

条件 ① >  
1 個の条件が選択されました

アクセス制御

許可 ① >  
0 個のコントロールが選択されました

セッション ① >  
0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 オン オフ

作成

許可

適用するコントロールを選択してください。

アクセスのブロック **設定 12**  
 アクセス権の付与

多要素認証を要求する ①

デバイスは準拠しているとしてマーク済みである必要があります ①

ハイブリッド Azure AD 参加済みのデバイスが必要 ①

承認されたクライアント アプリが必要です ①  
[承認されたクライアント アプリの一覧を表示します](#)

アプリの保護ポリシーが必要 (プレビュー) ①  
[ポリシーで保護されたクライアント アプリの一覧を表示します](#)

複数のコントロールの場合

選択したコントロールすべてが必要  
 選択したコントロールのいずれかが必要

選択

## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

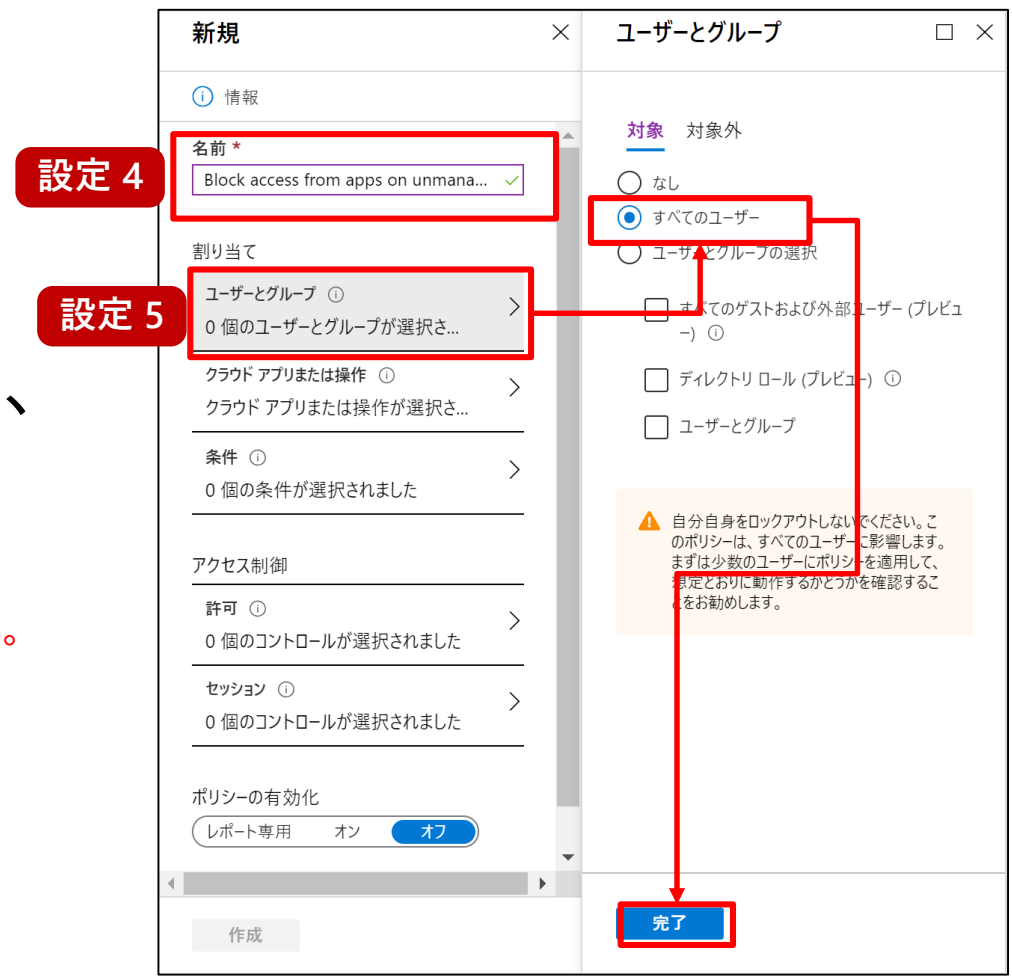
1. ブラウザー画面を開き、Azure Active Directory 管理センターの URL <https://aad.portal.azure.com> にアクセスします。
2. Azure Active Directory 管理センター画面で、[Azure Active Directory] - [セキュリティ] - [条件付きアクセス] の順にクリックします。
3. 条件付きアクセス画面で、[新しいポリシー] をクリックします。

## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

4. 新規画面で、ポリシーの名前として Block access from apps on unmanaged devices と入力します。

5. 新規画面で、[ユーザーとグループ] をクリックし、[すべてのユーザー] をクリックして、[完了] をクリックします。

※状況に応じて「すべてのユーザー」ではなくポリシーを適用されたいユーザーをご指定ください。



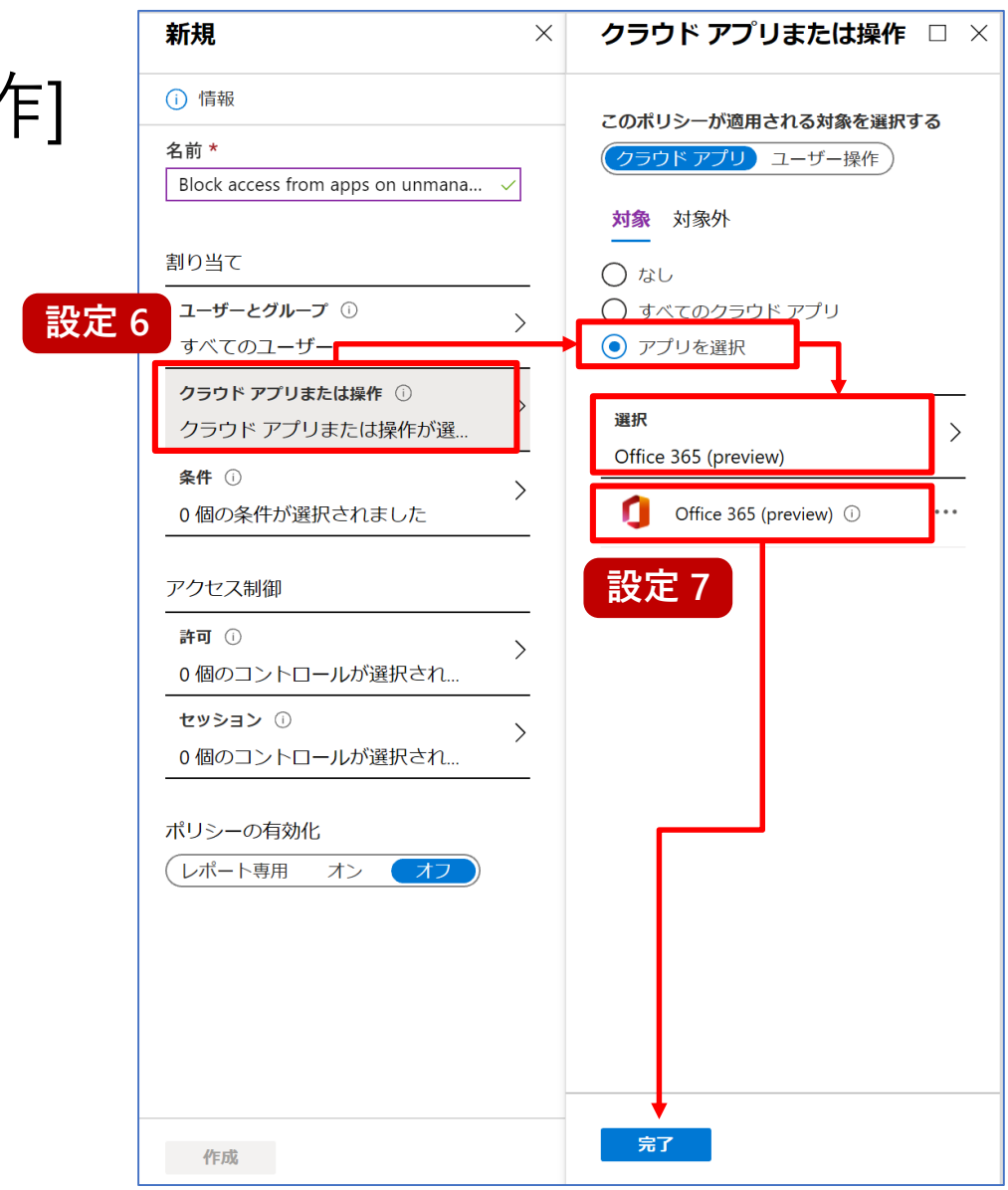
## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

6. 新規画面に戻り、[クラウド アプリまたは操作] をクリックし、[アプリを選択] をクリックして、[選択] をクリックします。

7. 選択画面で、Office365 (preview) にチェックを付け、[選択] をクリックします。

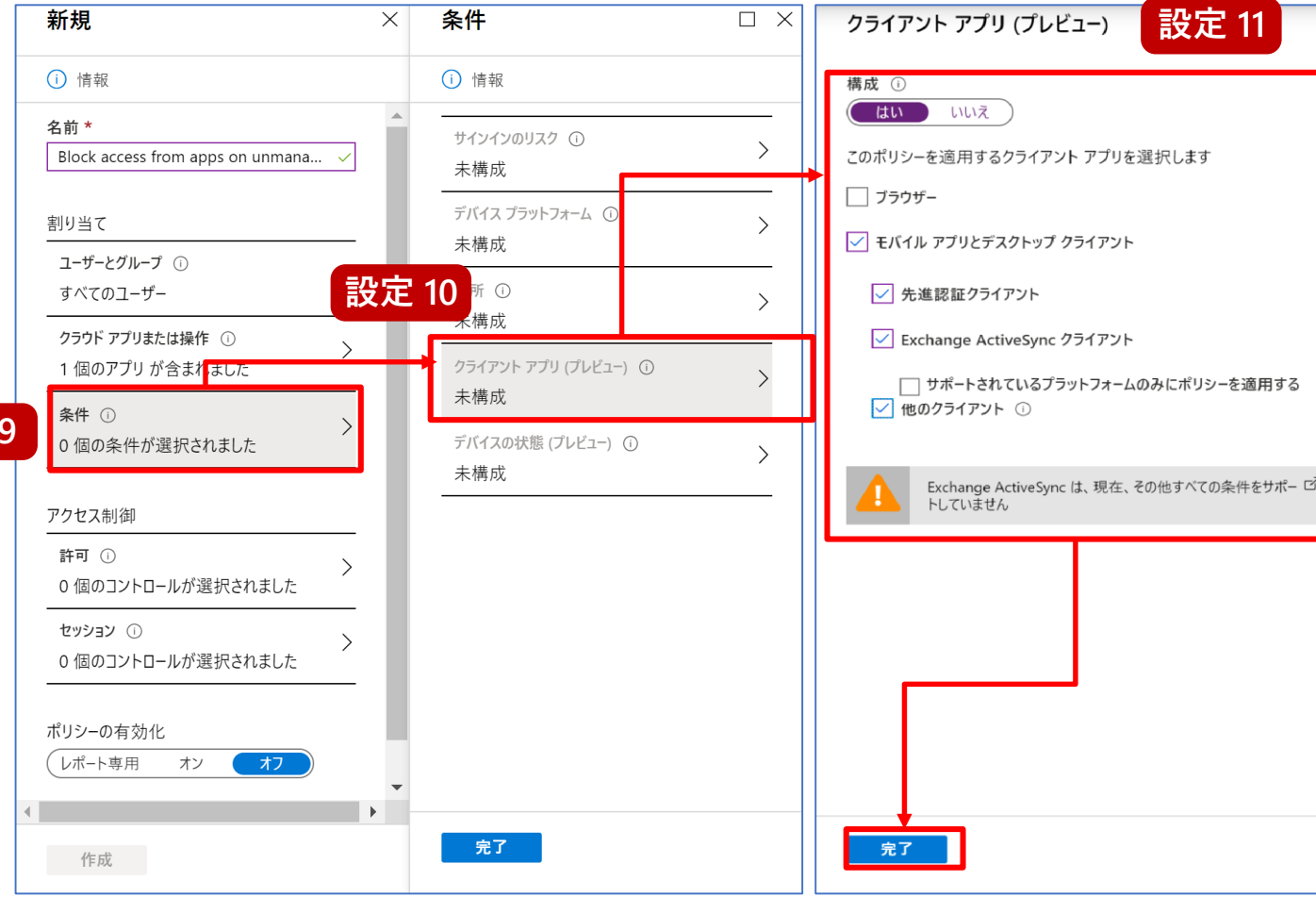
※Office 365 (preview) を選択した場合は Teams、SharePoint Online、Exchange Online などの各コンポーネントが対象となります。

8. クラウド アプリまたは操作画面で、[完了] をクリックします。



## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

9. 新規画面で、[条件] をクリックします。
10. 条件画面で、[クライアント アプリ (プレビュー)] をクリックします。
11. クライアント アプリ (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、下記にチェックをし [完了] をクリックします。
  - [先進認証クライアント]
  - [Exchange Active Sync クライアント]
  - [他のクライアント]



## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

12. 条件画面で、[デバイスの状態 (プレビュー)] をクリックします。
13. デバイスの状態 (プレビュー) 画面で、[構成] 欄から [はい] をクリックし、[対象外] をクリックして、[ハイブリッド Azure AD 参加済み デバイス] 欄と [デバイスは準拠としてマーク済み] 欄にチェックを付け、[完了] を 2 回クリックします。

※ 社内ネットワーク利用時をポリシーの適用対象外にしたい場合は P.59 をご参照ください。

この設定で「会社で管理する端末以外の端末からアクセスした場合」という条件を設定しました

設定 12

設定 13

完了

完了

## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

14. 条件画面で、[デバイスプラットフォーム] をクリックします。

15. デバイスプラットフォーム画面で、[構成] 欄から [はい] をクリックし、[対象] 欄の [デバイスプラットフォームの選択] で [Windows][macOS] チェックを付け、[完了] をクリックします。

条件

① 情報

サインインのリスク ① >

未構成

**設定 14**

デバイスプラットフォーム ① >

未構成

場所 ① >

未構成

クライアントアプリ (プレビュー) ① >

1 が含まれました

デバイスの状態 (プレビュー) ① >

すべてのデバイスの状態 を含め...

完了

デバイスプラットフォーム

選択されたデバイスプラットフォームにポリシーを適用します。  
詳細情報

**設定 15**

構成 ①

はい いいえ

対象 対象外

任意のデバイス

デバイスプラットフォームの選択

Android

iOS

Windows Phone

Windows

macOS

完了



## ② 非管理 PC の Office アプリからの Office 365 アクセスのブロック

16. 新規画面で、[許可] をクリックします。

17. 許可画面で、[アクセスのブロック] 欄にチェックをつけて [選択] をクリックします。

18. 新規画面で、[ポリシーの有効化] 欄を [オン] にし、[作成] をクリックします。

The screenshot shows the configuration process for blocking Office 365 access from unmanaged devices. It consists of two main windows: '新規' (New) and '許可' (Permissions).

- 新規 (New) Window:**
  - 名前 \***: Block access from apps on unmana... ✓
  - 割り当て**: ユーザーとグループ (すべてのユーザー), クラウド アプリまたは操作 (1 個のアプリが含まれました), 条件 (1 個の条件が選択されました)
  - アクセス制御**: 許可 (0 個のコントロールが選択されました), セッション (0 個のコントロールが選択されました)
  - ポリシーの有効化**: レポート専用, **オン**, オフ
  - 作成** button
- 許可 (Permissions) Window:**
  - 適用するコントロールを選択してください。
  - アクセスのブロック** (設定 17)
  - アクセス権の付与
  - 多要素認証を要求する (オフ)
  - デバイスは準拠しているとしてマーク済みである必要があります (オフ)
  - ハイブリッド Azure AD 参加済みのデバイスが必要 (オフ)
  - 承認されたクライアント アプリが必要です (承認されたクライアント アプリの一覧を表示します)
  - アプリの保護ポリシーが必要 (プレビュー) (ポリシーで保護されたクライアント アプリの一覧を表示します)
  - 複数のコントロールの場合:
    - 選択したコントロールすべてが必要
    - 選択したコントロールのいずれかが必要
  - 選択** button (設定 18)

# ③ Azure AD の条件付きアクセスの社内ネットワーク利用時の除外設定

本手順で作成した Azure AD の条件付きアクセスの各ポリシーの適用対象として社内の IP アドレスを除外する場合は、それぞれのポリシーの [条件] の [場所] から社内ネットワーク利用時をポリシーの適用対象外とすることも可能です。状況に応じて作成したポリシーへの追加設定を実施してください。

社内の IP アドレスをポリシーの適用対象から除外する設定の例

社内ネットワーク (信頼できる場所) の登録手順例

信頼できる場所としてマークするにチェック

19.168.0.0/24 などの社内のプライベート IP アドレスの登録ではなく、社内のインターネット接続に利用されるパブリック IP アドレスを登録します。(CIDR 形式の IP v4 アドレス範囲)

# Appendix 2 : 推奨構成プランの推奨設定

---

- 非管理 PC の Teams クライアント利用のブロック

# 設定手順

- ① 非管理 PC の Teams クライアント利用のブロック

# ① Microsoft Cloud App Security でアクセスポリシーを設定

1. Cloud App Security 管理ポータル画面で、左上のボタンをクリックし、[制御] - [ポリシー] をクリックします。
2. ポリシー画面で、[ポリシーの作成] - [アクセス ポリシー] をクリックします。



# ① Microsoft Cloud App Security でアクセスポリシーを設定

3. アクセスポリシーの作成画面で、ポリシー名に [Block Teams Client – Unmanaged PC] を入力します
4. 一致するアプリの条件に [Microsoft Teams] を指定します。



# ① Microsoft Cloud App Security でアクセスポリシーを設定

5. [+] ボタンから以下の条件を追加します。
- [クライアントアプリ]
  - [が次と等しい]
  - [モバイルとデスクトップ]

アクセスポリシーにより、リアルタイム監視と、クラウド アプリへのユーザー ログインの制御が可能になります。

ポリシー名 \*

Block Teams Client - UnManaged PC

ポリシー重要度 \*      カテゴリ \*

High      アクセス制御

説明

次のすべてに一致する アクティビティ

× デバイス      タグ      が次に等しくない

準拠している、ドメイ...

× アプリ      が次と等しい      Microsoft Teams

× クライアント アプリ      が次と等しい      モバイルとデスクトップ

設定 5

# ① Microsoft Cloud App Security でアクセスポリシーを設定

6. 画面を下にスクロールし、アクション [ブロック]を選択します。

7. [作成] をクリックします。

The screenshot shows the Microsoft Cloud App Security console interface. The title bar reads "Cloud App Security". The main content area is titled "アクション" (Action) and contains the following settings:

- アクション**  
ユーザー アクティビティがポリシーに一致した場合に適用されるアクションを選んでください。
- テスト  
ログイン アクティビティを監視します
- ブロック** **設定 6**  
可能な場合、既成のブロックメッセージが表示されます
- ブロックメッセージのカスタマイズ ①

The "アラート" (Alerts) section is also visible:

- 一致するイベントごとにポリシー重要度に応じたアラートを作成する  
既定の設定として保存 | 既定の設定に戻す
- アラートをメールで送信 ①
- アラートをテキストメッセージとして送信する ①
- 日次アラート制限: 5
- Power Automate にアラートを送信する  
ブレイックを選択してください...

At the bottom of the page, there is a note: "これらの変更が有効になるまで、数分かかる場合があります。プライバシーに関する声明に記載されているとおりにお客様のデータを保護します。" To the right of this note, there are two buttons: "設定 7" (highlighted in red) and "作成" (highlighted in red), followed by a "キャンセル" button.





© 2020 Microsoft Corporation. All rights reserved.

本情報の内容 (添付文書、リンク先などを含む) は、Microsoft Digital Trust Security Alliance 開催日 (2020 年 3 月 25 日) 時点のものであり、予告なく変更される場合があります。本コンテンツの著作権、および本コンテンツ中に出てくる商標権、団体名、ロゴ、製品、サービスなどはそれぞれ、各権利保有者に帰属します。